

AIR WAR COLLEGE

AIR UNIVERSITY

HIGH POWER MICROWAVES ON THE FUTURE BATTLEFIELD:
IMPLICATIONS FOR U.S. DEFENSE

by

Robert J. Capozzella, Lieutenant Colonel, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

17 February 2010

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the U.S. government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Disclaimer	i
Table of Contents	ii
List of Figures.....	iii
Biography.....	iv
Abstract.....	v
Introduction.....	1
HPM Weapons' Background Information	2
HPM Weapons' Capabilities, Today and in the Future.....	7
Implications for the U.S.....	11
Recommendations	13
Countermeasures	13
Deterrence	15
Conclusion	19
Notes	20
Bibliography	26

Illustrations

Figure 1. Electromagnetic Spectrum.....	2
Figure 2. Cutaway view of an explosive-driven HPM system	3
Figure 3. Lethal Footprint	6
Figure 4. Ranets-E Proposed Configuration	8
Figure 5. HPM vs. EMP.....	15
Figure 6. Deterrence Calculation	15

Biography

Lieutenant Colonel Robert J. Capozzella hails from Sackets Harbor, New York. He graduated from the United States Air Force Academy in 1989 with a Bachelor of Science Degree in Mathematical Sciences. He went on to earn Master's Degrees in Aeronautical Sciences from Embry-Riddle Aeronautical University in 2001 and Operational Sciences from Air University in 2002. He is also a Graduate of Squadron Officer School, Air Command and Staff College, and Air War College.

Lieutenant Colonel Capozzella graduated from pilot training from Sheppard Air Force Base in 1990. Following pilot training and Lead-in Fighter Training, he was assigned to the 524th Fighter Squadron, Cannon AFB, NM flying the F-111. During this assignment, he attended and was a distinguished graduate of the United States Air Force Weapons School.

Following his tour at Cannon, Lieutenant Colonel Capozzella was selected for an exchange tour with the Royal Australian Air Force. During this assignment, he served as an R/F-111C instructor pilot and the Chief of Weapons and Tactics Development for RAAF 1 Squadron based at Royal Australian Air Force Base Amberley, Australia. Upon his return in 1998, he cross-trained to the F-15E at Seymour Johnson Air Force Base with a follow-on assignment to Royal Air Force Lakenheath, England. He was assigned to the 492nd Fighter Squadron where he served initially as the Chief of Weapons and Tactics and his tour culminated as Flight Commander.

In 2002, after attending Air Command and Staff College, Lieutenant Colonel Capozzella was assigned to the Tactical Leadership Programme, Florennes Air Base, Belgium where he served as the Flying Branch Chief of Air to Ground Tactics and Flying Branch Director of Operations.

In 2005, he was assigned to the 366th Fighter Wing at Mountain Home Air Force Base as an F-15E instructor pilot and Chief of Wing Weapons and Tactics.

In 2006, he was assigned to Vance Air Force Base as a T-6 instructor pilot and Director of Operations of the 33d Flying Training Squadron. He culminated his tour as the commander of the 33d from 2008-2009. He is currently a student at Air War College at Maxwell AFB Alabama.

Lieutenant Colonel Capozzella is a command pilot with over 3,000 hours, including over 1000 hours in both the F-111 and F-15E and over 300 combat hours in support of Operations PROVIDE COMFORT, NORTHERN WATCH, SOUTHERN WATCH, DELIBERATE FORCE, and ALLIED FORCE. His decorations include the Defense Meritorious Service Medal, Meritorious Service Medal with one device, Air Medal with two devices, Aerial Achievement Medal with 2 devices and various unit, campaign and individual awards.

Abstract

One of the U.S. Military's greatest strengths, integration of technology, may soon turn into its greatest liability as recent advances in the area of high power microwave (HPM) weapons are garnering interest around the world. Current U.S. military strategy is to develop and maintain its superiority through the leveraging of information technology, but as recent conflicts have shown, potential enemies are likely to attack asymmetrically. HPMs against electronics is an asymmetric avenue to negate the technological advantage of the U.S. Therefore, nations, groups, and/or individuals will likely seek to use HPM weapons against the U.S. This paper argues that the U.S. should continue to research and develop HPM weapon systems that target electronics, discern how an enemy may use them against us, develop countermeasures, and deter HPM offensive uses, particularly those that can have catastrophic results.

I. Introduction

One of the U.S. Military's greatest strengths, integration of technology, may soon turn into its greatest liability as recent advances in high power microwave (HPM) weapons are garnering interest around the world. The scientific and military communities have known the potential weapons effects of HPM or radio frequency (RF) energy since the 1930s with the development of radar and microwave systems.¹ Research into RF weapons technology expanded in the Soviet Union in 1949.² The U.S. followed with electromagnetic pulse (EMP) research in the 1960s.³ However, it was not until 1983 that the U.S. truly started researching RF technology as a directed energy weapon.⁴ While the United States, Russia, and Ukraine continue to lead in this technology field, other nations have become interested. Today, the United Kingdom, France, Germany, Australia, Japan, China, Sweden, India, Pakistan, South Korea, Taiwan, Lithuania, and Israel have HPM programs at various levels of development.⁵ Some of them, particularly China, are not far behind as they jump-started their programs with HPM technology from Russia and Ukraine.⁶

Three trends can explain the increased attention on HPMs. The first is advances in power source technology. Improved generators, batteries, and HPM sources have enabled power output in a smaller and lighter package.⁷ Second, new electronic components in military and consumer systems are more susceptible to RF weapons because the transistors on their computer chips are smaller and more densely packed.⁸ Third, the U.S. and her allies are dependent on these electronic systems.⁹ Therefore, HPM weapons may affect electronic systems, with the U.S. and its military particularly vulnerable to these weapons.

Current U.S. military strategy is to develop and maintain its superiority through the leveraging of information technology, but as recent conflicts have shown, potential enemies are

likely to attack asymmetrically.¹⁰ HPMs against electronics is an asymmetric avenue to negate the technological advantage of the U.S. Therefore, nations, groups, and/or individuals will likely seek to use HPM weapons against the U.S. to gain an advantage.

To prepare for this possibility, the U.S. should continue to research and develop HPM weapon systems that target electronics, discern how an enemy may use them against the U.S., develop countermeasures, and deter HPM offensive uses, particularly those that can have catastrophic results.¹¹ To understand why, this paper first provides background information on how HPM weapons work, their advantages, and disadvantages. Second, it examines these weapons' current and future capabilities. It also analyzes who may use these weapons in the future. From these, the paper will then examine the impact of HPM weapons on the U.S. and its military. Finally, this paper will make recommendations regarding defense of the U.S. in a future with HPM weapons in the hands of its enemies.

II. HPM Weapons' Background Information

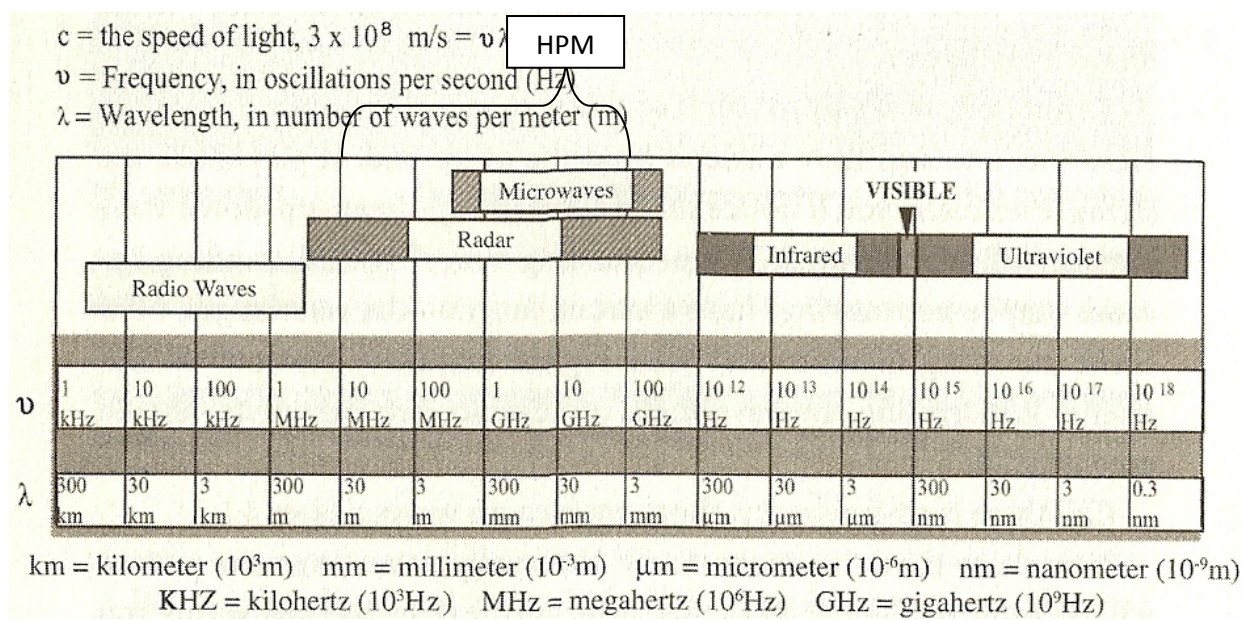


Figure 1. Electromagnetic Spectrum¹²

An HPM weapon is a “device designed to disrupt, degrade, or destroy targets by radiating electromagnetic energy in the RF spectrum, typically between 10 MHz [megahertz] and 100 GHz [gigahertz] (figure 1).”¹³ The basic elements of an HPM device are a power source, a microwave source, and a transmitter (figure 2). They determine the HPM beam’s characteristics, and power. These along with the target’s vulnerabilities, determine the effective range. Depending on the beam the device produces, the scientific and engineering community further divides HPM weapons into two categories, narrow-band, and ultra-wideband. A narrow-band device emits all its energy within one percent of the central frequency (10s to 100s of megahertz depending on the frequency) whereas an ultra-wideband device disperses its energy over a bandwidth from 100s of megahertz to several gigahertz wide.¹⁴ This distinction will be important next in the discussion on how HPMs affect electronic equipment.

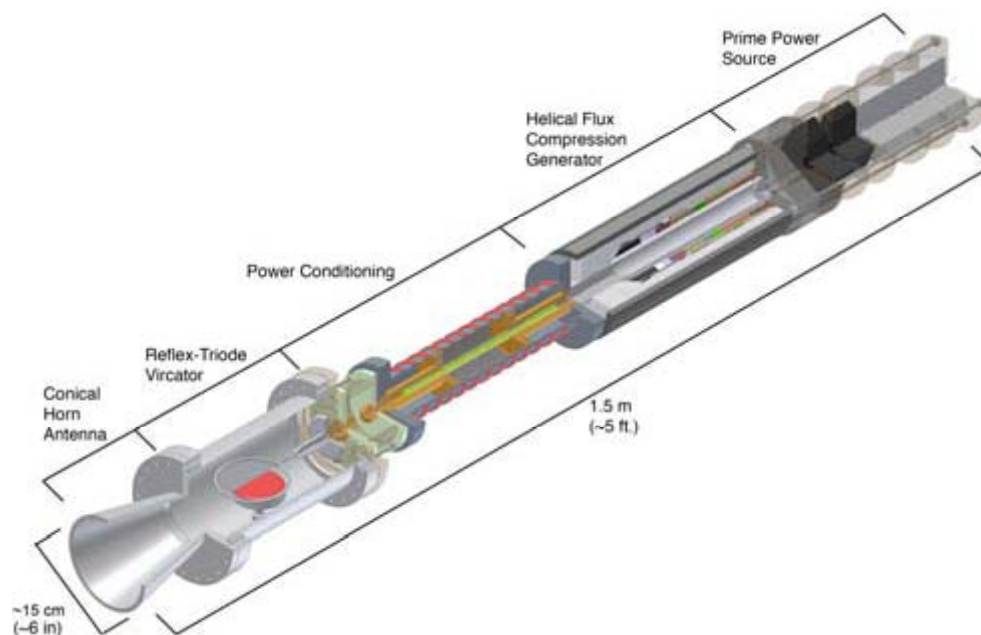


Figure 2. Cutaway view of an explosive-driven HPM system¹⁵

HPM weapons disrupt, degrade, or destroy targets by overwhelming the target’s ability to reject or disperse the incoming RF energy in two ways.¹⁶ First, the RF energy can cause

molecular heating to the point where components melt, but this requires high power over a long duration, which is hard to accomplish and highly dependent on component composition.¹⁷ The more efficient and primary mechanism for an attack is electrical stimulation in the target's electronics. This occurs when the RF energy from the HPM enters a circuit and produces stray currents and voltages.¹⁸ The exact effect on the target depends on several factors to include the beam's characteristics (range, frequency, power level, pulse width, etc) and target composition (materials, shielding, electronic design, entry points, etc).¹⁹

There are two pathways into an electronic system. First, RF energy enters the system through a component or sensor designed to receive the energy like a radar antenna, known as front-door coupling. As one can see from figure 1, HPMs are in the same part of the electromagnetic spectrum as communications and radar systems. These systems receive and amplify weak signals, which can enhance an HPM's ability to overwhelm the system especially if they are in the same frequency band. Because these systems filter out-of-band signals, pulsed narrow-band HPMs work best for front-door coupling.²⁰ Second, HPMs can enter through other apertures or cracks that allow the energy to diffuse into the system, known as back-door coupling. Any electrically conductive material can act like an antenna for HPMs. Once the stray currents and voltages enter the system, they disrupt or destroy the individual electrical components. Ultra-wideband devices are ideal for back-door coupling since their wide range of wavelengths take advantage of multiple coupling mechanisms and points of entry. This is advantageous when one is not certain of a target's composition a priori.²¹

HPM weapons provide other unique advantages and effects, which is why the U.S. and others are pursuing them. First, HPM weapons can minimize collateral damage. These weapons produce little or no physical damage and are therefore ideal for targeting in an urban

environment. Second, they have a deep magazine. As long as they have a power source, they can shoot multiple times and engage multiple targets. This can mean reduced logistics costs and lower costs per target relative to conventional weapons. Third, they operate at the speed of light. Fourth, as stated earlier, the effects are scalable. These can be temporary or permanent depending on the energy deposited on the target.²² Fifth, repairing a system after an attack is difficult since one cannot say with 100 percent reliability that the system is fully functional without checking each component. Sixth, weather and the atmosphere have little effect on HPMs. Seventh, for electronic attack, HPMs can jam a system without knowing the RF output of the targeted system, and the effects last even after the HPM signal is not present.²³ Eighth, they have the potential to affect deeply buried bunkers by targeting vulnerable electronic systems that support the bunker, i.e. communications, power, and air ventilation systems. The bunker may as well be a tomb if it cannot connect to the outside world.²⁴ Finally, they can be an area weapon, affecting every vulnerable system within the lethal footprint. The footprint depends on the HPM's power output, range from the target, and beam divergence (figure 3).²⁵ However, just like conventional weapons, collateral damage can occur if friendly or civilian electrical systems are also in the footprint, which also makes this a limitation.

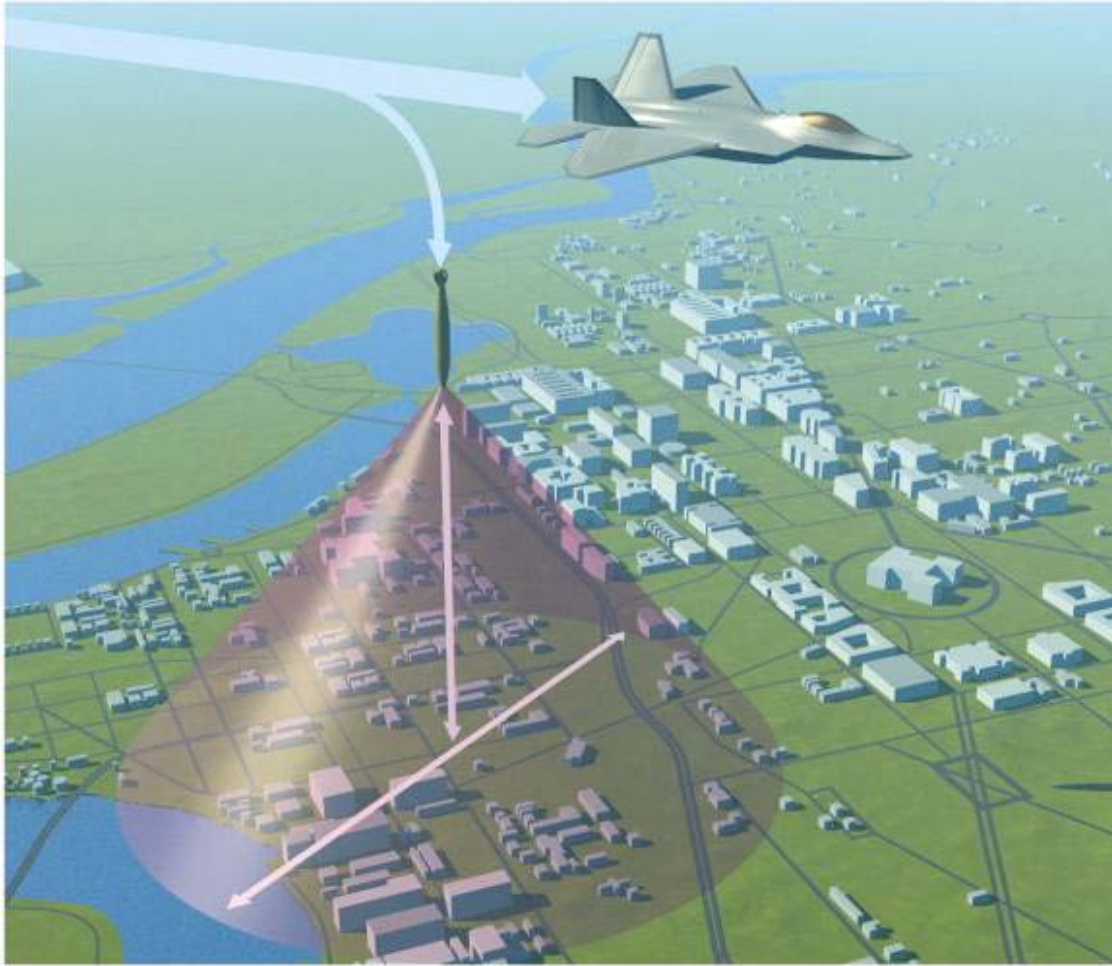


Figure 3. Lethal Footprint²⁶

There are three main limitations of HPMs. First, HPM weapons affect all unprotected electronic systems within its lethal footprint including civilian and friendly systems.²⁷ Second, it is difficult to assess the result of an attack since there are no signs of physical destruction. Just because a system stops operating or emitting does not mean it was because of the HPM attack. Likewise, a system can continue to emit, but not be functional.²⁸ Third, they can be range limited. For an HPM weapon system, range is proportional to both power output at the antenna, and antenna size. As the power and/or aperture increases, the HPM weapon can deliver more RF energy on the target at farther ranges.²⁹ However, a beam at sufficiently high power levels and duration causes the atmosphere at the aperture to become plasma. As long as the HPM pulses

continue, the plasma density increases, eventually reaching the point where the plasma reflects and absorbs the RF energy rendering the beam ineffective and creating a shielding problem for the delivery platform.³⁰ Scientists and engineers refer to this phenomenon as “atmospheric breakdown.”

Some solutions to these limitations are as follows. First, properly shield friendly systems, and/or plan for them and civilian systems before attacking with HPM weapons. Second, develop new sensor technology and techniques for measuring second and third order effects to corroborate the results and enhance attack assessment. Third, once atmospheric breakdown occurs, the only way to increase the range is to increase the aperture, which may not be possible for portable or airborne designs. The paper will cover these and other solutions in more detail in the next section when discussing future systems and trends.

III. HPM Weapons’ Capabilities, Today and in the Future

This section first looks at current HPM systems, then HPM and related technological trends. Using this information, this section examines what the HPM threat could be by 2035.

Three unclassified HPM weapon systems fielded today target electronic systems. The first system is the U.S. military’s NIRF (neutralizing improvised explosive devices (IEDs) with RF). It produces an HPM beam to neutralize or destroy an IED through its wiring. Second, the U.S. army has “Warlock Green” and “Warlock Red” to target the fusing and proximity sensors in artillery rounds. Similar to these systems is the German DS110B suitcase device designed to disrupt computers and electronic systems within its effective radius. All of these systems have one thing in common; they are all relatively short range, effective out to only 100s of meters.³¹

There are also a myriad of systems in various stages of development that should be ready in the near future. These include a vehicle stopper, HPM bombs or e-bombs, and anti-aircraft systems.³² The U.S. Army and several law enforcement agencies are developing HPMs to stop vehicles through attacking the engine's ignition system.³³ Unlike this system, e-bombs have garnered little attention even though they are feasible today. The reason is that current designs have a very short effective range.³⁴ As for the anti-aircraft systems, Russia is researching and trying to sell the Ranets-E and Rosa-E (figure 4). The first is a point defense system designed to target the electronics of modern aircraft; the second is an aircraft defensive system that targets the radar of enemy aircraft. These are still in development, however based on the advertised beam output; their range is promising against unshielded systems but otherwise limited.³⁵ The final system in development to discuss is Raytheon's Vigilant Eagle. The system protects aircraft during takeoff and landing by using HPM systems around an airport to disrupt the guidance of shoulder-fired surface-to-air missiles (SAM). While each HPM device is short-range, Raytheon is planning for the system to create a dome of protection around an airport in an integrated defensive grid of multiple systems.³⁶ Vigilant Eagle will require huge amounts of power and will be quite large.



Figure 4. Ranets-E Proposed Configuration³⁷

While the above systems have limited capabilities, recent trends in power sources are likely to improve these designs. For larger systems, primary power sources and pulse conditioners are increasing in power and efficiency. One-terawatt generators are already available.³⁸ For portable applications, they are decreasing in size and weight while power density is increasing. There are advances in battery design, compact pulse generators, and ultra-capacitors. The most promising advances are lithium-ion batteries, and nano-material integration with projected densities of 120 to 280 watt-hours/kilogram.³⁹ There are also advances in ultra-wideband flux compression generators with lab tests achieving 550MW to 1.2GW peak power for those pursuing e-bombs.⁴⁰ One area that still needs work is reducing the size and increasing the efficiency of pulse-power converters. Some possible solutions are nanotechnology advances in dielectrics, solid-state, and pseudo switches.⁴¹

Just as advances in power sources are trending to be more powerful, compact, and efficient, microwave sources and transmitters are trending in the same direction. Previous microwave sources were running at approximately ten percent efficiency, but recent designs are approaching 50-percent conversion efficiency.⁴² One can see these efficiency increases across a wide range of microwave source technologies.⁴³ For transmitters/antennas, planar arrays and solid-state switching is allowing more efficient and compact designs. The most interesting of these designs integrates the antenna into the skin of the system. The aperture can then be as large as the delivery platform, which is essential for airborne systems where space is a premium.⁴⁴ The one limit that remains is atmospheric breakdown at high power output. Besides increasing the actual antenna's aperture, scientists are researching the concept of phase-locking, combining multiple transmitters, to increase the effective aperture size and power on target.⁴⁵

Unless there is an unforeseen breakthrough to solve atmospheric breakdown, HPM characteristics, current capabilities, and research points to two outcomes for future HPM weapons applications. First, for applications like point defense where the target is traveling to the HPM weapon and size is not a limiting factor, one can increase the range by either increasing the aperture size of the transmitter or combining multiple transmitters as mentioned above. Ranets-E and Vigilant Eagle are examples of these types of systems. For portable compact or airborne systems where the HPM payload travels to the target, smaller systems will depend on other technologies like a UCAV to get within range of the target. The USAF's CHAMP is the prototype for a UCAV armed with an HPM payload.⁴⁶

Based on these current capabilities and trends, several HPM devices will be available for defensive and offensive uses by 2035. Defensive systems will include fixed and mobile, land or ship-based systems that target the electronics of attacking missiles, bombs, and aircraft as part of an integrated air or point defense. In addition, airborne defensive systems will include self-protection suites on aircraft to target enemy radars and missiles, and HPM warheads on missiles to target attacking enemy aircraft and missiles at range. Offensive HPM weapons will include precision-guided e-bombs, cruise missiles, unmanned or manned aircraft with integrated HPM weapons capable of multiple shots and engagements, and covert suitcase and vehicle-borne HPM weapons.⁴⁷ These offensive weapons will be able to target any electronic system, but enemies will likely use them to target communications, radar, ships, satellites, infrastructure, and command and control systems.

Overall, these weapons will likely be attractive to nation-states, groups, and individuals who become increasingly aware of the U.S. reliance on electronic information systems.⁴⁸ The

following are two possible examples of how enemies could use these HPM weapons against the U.S., and show why the U.S. should prepare for them.

In the first example, a nation uses HPM weapons to defend against a U.S. attack, targeting communications, standoff, and precision capabilities thereby negating U.S. technological superiority. The enemy targets U.S. forward operating bases and ships with HPM missiles and UCAVs, or vehicle-borne HPM devices, wiping out electronics and communications so the U.S. cannot launch or control operations in the theater. The enemy also uses its HPM defensive systems to target attacking aircraft, missiles, and bombs. As a result, the U.S. is unable to operate in the region, weapons miss their targets, and collateral damage and public outcry become an increasing problem.

In the second example, an enemy nation, group, or individual targets a vulnerable U.S. infrastructure or business. For instance, they use multiple vehicle-borne weapons to target critical nodes of the U.S. electrical grid. Depending on the severity of the attack, it could take from 1.5 to 33 months to repair the systems.⁴⁹ Terrorists or criminals might also use an improvised e-bomb causing death and destruction in the immediate area while also disrupting the electronics in a wider area affected by the HPM device, e.g. Wall Street.

IV. Implications for the U.S.

HPM weapons could have a profound impact on the U.S. military. On the battlefield, U.S. costs, casualties, and collateral damage would increase while weapons accuracy would decrease. All these would affect military effectiveness, as well as erode U.S. public and international support, which would influence the decision to use military force. In addition, an enemy that could target U.S. forward operating bases and its standoff strike capabilities could

negate U.S. military global power projection and threaten her ability to protect interests abroad. Operations would have to change to account for the reduced effectiveness, degraded command and control, and increased risk.

This not only affects military operations, but also the ability of the U.S. Government to deter or compel others. Without military access to a region, the U.S. would be reliant on other forms of national power without military force to back them up, making them less effective. The U.S. would also be more dependent on regional partners and international institutions that might not always act in her best interest. In addition, an enemy might not limit their attacks to deny the U.S. from using its military and conducting operations abroad. They could also use HPM weapons against homeland assets to influence the U.S.

An enemy could inflict significant damage to U.S. infrastructure and its economy with several relatively simple HPM weapons as mentioned earlier. The U.S. is dependent on automation and information technology in government functions, infrastructure, and the commercial sector. It is hard to imagine any of these continuing to function without commercial electronics and computers. Even so, many of these critical systems remain vulnerable to HPMs with few or no backups.⁵⁰

In summary, the U.S. would lose freedom of action, and the ability to influence other nations, groups, and individuals acting on the international stage. In addition, an HPM attack could increase the costs for the U.S. In effect, an enemy with these weapons may be able to deter or compel the U.S. and make U.S. national strategy less effective.

V. Recommendations

The U.S. must maintain the ability to use military force and overall freedom of action to defend her interests in a future with HPM weapons. Therefore, the U.S. must be able to defend against HPM weapons as well as deter enemies from using them offensively against the U.S.

Countermeasures

Before one can decide how to defend against a particular threat, one must understand the threat and its impact. Therefore, there are three keys to developing effective countermeasures to HPM weapons. First, the U.S. must continue to research and develop these weapons to appreciate their potential effects and to know when their use is advantageous. Second, the U.S. must continue to monitor potential adversaries to determine their HPM capabilities and intentions. As with all intelligence gathering, this is difficult, but critical for planning a response. Third, the U.S. must test and ascertain the vulnerabilities of critical infrastructure, national, and military systems.⁵¹ This costly and time-consuming venture requires testing against the full spectrum of HPM frequencies to include front-door and back-door entries. This information will determine the appropriate defenses.

Defending against an HPM attack entails a combination of active and passive measures. First, detect and destroy HPM weapons before they are in range. This is no different from defending against conventional weapons. It requires continued investment in sensors and surveillance to detect small, low cross-section targets like cruise missiles and UCAVs as well as mobile land and sea-based HPM platforms. In addition, the U.S. needs to develop weapons that are not susceptible to HPMs in which to target these platforms. A solution should incorporate laser-based defenses because they operate at the same speed as HPMs but with greater range.

Second, shield or harden critical infrastructure, military systems, and components. Faraday cages, fiber-optic cable, optical computing, fast acting diodes, filters, and nano-materials to shield entry lines and components are just a few of the technologies and techniques that the U.S. should explore and develop.⁵² Many of these techniques are similar to nuclear EMP countermeasures, but require changes to account for the different characteristics and shorter wavelengths of HPMs (figure 5). For some systems, it may not be possible or cost effective to shield them completely. One cannot put a faraday cage on every item, however every line in/out, crack, or aperture is a potential entry point that needs protection. For fielded systems, retro-hardening is difficult and expensive.⁵³ In addition, maintaining the shielding in the field is challenging as wear and tear produces cracks and apertures for HPMs to infiltrate.⁵⁴ Therefore, the third measure is when the other defenses fail; develop backup systems and responses to mitigate the cost and risk of an attack. The U.S. must detect the attack, have procedures to operate without the damaged critical system(s), and then quickly repair or replace the system(s). For the U.S. military, this includes developing techniques, tactics, and procedures to operate without some of its high tech capabilities, and to train to these scenarios in exercises and war games. Unfortunately, the U.S. military rarely trains to this level of degradation, but it is essential or these skills will not be there when needed.⁵⁵ These countermeasures are also essential elements in deterring HPM weapons, but are not sufficient on their own.

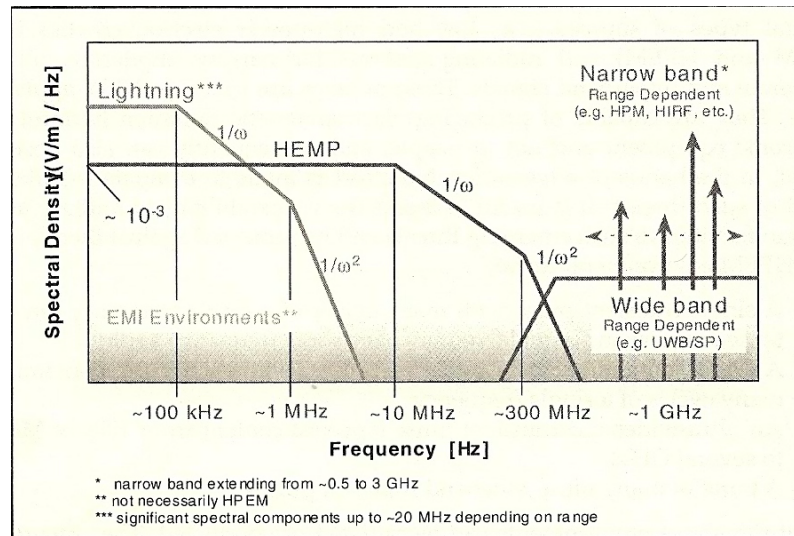


Figure 5. HPM vs. EMP⁵⁶

Deterrence

For this discussion, deterrence is a coercive strategy that prevents an opponent from taking an action because of the “fear of unacceptable punishment or denial of victory.”⁵⁷ Deterrence is a cost-benefit analysis based on whether the perceived benefit of an action is greater than the perceived cost. Therefore, one can deter an enemy by either increasing the perceived costs through threats of punishment, or by denial of the perceived gain. The following are simplified equations that illustrate the cost-benefit thought process.

$$\begin{aligned} \text{Cost} &= (\text{Blood} + \text{Treasure} + \text{Resources} + \text{Legitimacy}) \times \text{Probability of incurring cost} \\ \text{Benefit} &= (\text{Gain}) \times \text{Probability of Success} \\ \text{Successful Deterrence occurs when } \text{Cost} &> \text{Benefit} \end{aligned}$$

Figure 6. Deterrence Calculation⁵⁸

For deterrence to work effectively, one must consider its essential elements and assumptions. First, deterrence requires the capability to increase the cost and/or lower the gain for the enemy. Second, such capability must be credible. Third, one must communicate the

proposed action to the opponent and they must accurately understand it.⁵⁹ Likewise, one needs to understand the enemy's calculus to affect it. The major assumption is that the opponent is rational, i.e., they do a cost-benefit analysis and decide to do what is in their best interest. Another assumption is that deterrence operates between all actors who have a rational calculus that is vulnerable to U.S. actions, whether they are nation-states, groups, or individuals. While some individuals may be nihilistic, this paper posits that unless such an actor is self-supporting, it is possible to deter rational sponsors of these individuals.⁶⁰

The U.S. should focus on deterring the offensive use of HPMs since it cannot deter their development or defensive use. The U.S. cannot deter the development of HPM weapons for three reasons. First, as stated earlier, the U.S. is not the only nation developing HPM systems. Second, HPM components have commercial as well as military uses.⁶¹ Finally, HPM components are not internationally controlled, which makes tracking them difficult.⁶² The U.S. also cannot deter purely defensive uses as in point or integrated air defense. In accordance with the UN charter and other international agreements, all nations have an inherent right of self-defense. In addition, it is not feasible to prevent a nation from developing and deploying a system comprised of uncontrolled components confined within its borders. However, if the U.S. should decide to use military force, it must have weapons to either destroy the HPM defensive systems first, and/or have weapons and tactics that are not susceptible to them.

Deterrence of offensive uses of HPM weapons should have both a denial and punishment strategy to give the best chance of success for three reasons. First, an enemy may choose to use HPMs against the U.S. even though the perceived gain is low, hence the U.S. should also have the capability to increase the perceived cost. Second, future enemies will not only be nations, but also non-state actors, including groups or individuals. A denial strategy can hedge against an

enemy that does not have interests or resources the U.S. can easily identify or hold at risk. Finally, the two strategies are not mutually exclusive. For example, developing weapons systems that are not susceptible to HPMs denies the enemy gaining an advantage from an HPM attack while also enabling U.S. forces the ability to strike enemy targets to increase the enemy's costs.

The basic requirements for each strategy are for the U.S. to have offensive and defensive HPM capabilities, accurate intelligence, and effective communications. As stated above, the U.S. must ascertain the adversary's capabilities and intentions as well as communicate to the adversary her capabilities and intentions. The ultimate goal would be complete transparency, i.e. perfect knowledge and clear communications on both sides so there are no misperceptions.

The denial strategy is the same as the countermeasures for HPMs covered earlier: detect and destroy HPM weapons before they reach their targets, harden the electronics of critical systems or remove the dependency on these vulnerable systems, and develop backup systems and mitigation responses. These actions will defend against an HPM attack as well as deny an enemy the benefit of an HPM attack. However, denial alone may not deter their use, so the U.S. must also have a punishment response.

Deterrence by punishment is a much more difficult problem. Deterrence by punishment first requires accurate detection and forensics to trace an attack to its origin so the U.S. can hold those responsible accountable. Second, the U.S. must have the capability and will to respond, which depends on the type and severity of the attack. It does not matter that the U.S. responds symmetrically or asymmetrically. It is only important that the enemy perceives that the response increases the cost beyond what they are willing to endure. Third, the U.S. must communicate

this response to the enemy. The key is for U.S. decision-makers to understand the enemy, their vulnerabilities, and their probable responses to U.S. actions or threats. In addition, U.S. decision-makers must consider the domestic and international public reaction. Therefore, the remaining question is what level of attack requires a response and of what type and severity.

It is beyond the scope of this paper to give recommended responses for every type of HPM attack.⁶³ However, this paper provides a range of possible responses to the lower and upper ends of the spectrum. In addition, this paper argues that only HPM attacks that can have catastrophic results require the U.S. to articulate a specific response.⁶⁴

At the lower end of the spectrum, there are HPM attacks against U.S. military equipment, bases and ships, and against individual businesses or nodes of a system, like a bank or an airport. Since these results mirror the damage sustained by an attack with conventional weapons, the U.S. should be consistent and respond in the same manner. Such attacks warrant a proportional response, ensuring the protection of U.S. territory, equipment, and personnel from further attack, and holding the attacker(s) accountable. Likewise, deterrence of HPM attacks below the catastrophic level should also fall within the realm of conventional deterrence.⁶⁵

At the catastrophic level, there are attacks with multiple HPM devices that result in the destruction of a critical U.S. system like the electrical power grid, air traffic control system, or financial sector. For example, an enemy uses several HPM devices to destroy a sector of the U.S. electrical power grid, putting millions of U.S. citizens at risk and costing up to \$770 billion in lost economic output.⁶⁶ The effects mirror a high altitude EMP attack and deserve a consistent response. Therefore, to deter such attacks, the U.S. should make it abundantly clear that an HPM

attack of this magnitude will result in a U.S. response with all measures at its disposal, up to and including nuclear weapons.⁶⁷

Conclusion

Although HPM weapons are not new, they have recently garnered more attention as advances in enabling technologies have made them more powerful and compact, and miniaturization has made modern electronics and computers more susceptible to them. The U.S. is particularly vulnerable to HPM weapons since her infrastructure, commercial, and military systems are heavily dependent on these information technologies. With enemies of the U.S. seeking to use HPM weapons to exploit this vulnerability, it is clear that the U.S. must prepare for this possibility.

Ultimately, the U.S. cannot afford to lose the ability to use military force and overall freedom of action to defend her interests in a future with HPM weapons. Therefore, the U.S. must develop effective defenses and retaliatory capabilities to deter HPM attacks, and should deterrence fail, have countermeasures that allow the U.S. to operate in this environment. To accomplish this, the U.S. must continue to research and develop these weapons, test and build systems that are not susceptible to HPMs, and develop techniques, tactics, and procedures to negate their effects.

Notes

¹ Hecht, *Beam Weapons*, 1. Gibilisco, *Physics Demystified*, 474-476. Radio frequency (RF) radiation is electromagnetic radiation with a wavelength of 100km to 1mm, which is a frequency of 3 KHz to 300 GHz, respectively (figure 1). RF can refer to electromagnetic oscillations in either electrical circuits or radiation through air and space. High power microwaves exist within this range and produce these phenomena associated with RF radiation. *Wikipedia*, s.v. “radio frequency,” http://en.wikipedia.org/wiki/Radio_frequency.

² Brunderman, *High Power Radio Frequency Weapons*, 2-3.

³ Wood, Lowell; Graham, William; Bernardin, Michael; Jakubiak, Stanley J.; Effect of Electromagnetic Pulse Attacks, Testimony before the House of Representatives Committee on Armed Services Subcommittee on Military Research and Development, 7 October 1999, available at http://commdocs.house.gov/committees/security/has280010.000/has280010_0.HTM as of February 8, 2010.

⁴ Benford, Swegle, and Schamiloglu, *High Power Microwaves*, 2-3, and Brunderman, 3. U.S. interest in HPM technology as a directed energy weapon increased because of Soviet advances in the late seventies, and President Reagan’s announcement of the Strategic Defense Initiative in 1983.

⁵ Robert L. Schweitzer, Lt Gen, US Army (Ret). *Radio Frequency Weapons and the Infrastructure*. Transcript provided from internet site <http://cryptome.org/rfw-jec.htm>. The list of countries comes from the above source as well as numerous articles and published works from databases (IEEE and DTIC), journals, and websites. Briefings and attendees at the 2007 and 2008 Directed Energy Symposiums confirm the continued interest by many of these countries.

⁶ “Foreign Help for High Tech Weapons.”

<http://www.globalsecurity.org/military/library/report/2004/04fisher/5hitech.html>, and Dr Ira W. Merritt. *Radio Frequency Weapons and Proliferation: Potential Impact on the Economy*. Transcript provided from internet site <http://cryptome.org/rfw-jec.htm>.

⁷ Benford, Swegle, and Schamiloglu, 46-49.

⁸ Ibid, 46-49. For modern unshielded computers, the threshold vulnerability level is very low. A fluence of 10^{-7} J/cm² will cause bit errors and disrupt the systems operation.

⁹ Ibid, 46-49.

¹⁰ Major, “Which Revolution in Military Affairs?” The Revolution in Military Affairs started in the 1990s. Quadrennial Defense Reviews of 1997 and 2001, concepts like Network Centric Warfare, and Joint Vision 2010 are illustrative of the beginning and current propensity for information technology in U.S. military operations.

¹¹ For this discussion, a catastrophic attack poses an existential threat, or can cause irreparable damage to the U.S. economy and/or political systems, or result in mass casualties.

¹² Beason, *The E-Bomb*, 28.

¹³ Ibid, 23.

¹⁴ Givri, *High-Power Electromagnetic Generators*, 29-32, and McCarthy, *Directed Energy and Fleet Defense*, 22. “High-power microwave devices typically operate at frequencies between 1-20 GHz with large pulse widths (on the order of one microsecond) and relatively narrow bandwidths (nominally one percent of the frequency, which equates to approximately 10 MHz at the lower end and as much as 100 MHz at the upper end). Ultra-wideband systems are characterized by narrow pulse widths of less than 100 nanoseconds and bandwidths that may

exceed 50 percent of the center frequency. Typical wideband devices have bandwidths that range from 200 MHz to 3 GHz.”

¹⁵ Neuber, Young, Elsayed, Dickens, Giesselmann, Kristiansen, and Altgilbers, “Compact High Power Microwave Generation,” 2.

¹⁶ Sowders, et al, *High Power Microwave (HPM) and Ultrawideband (UWB)*, 7.

¹⁷ David Schriner, *The Design and Fabrication of a Damage Inflicting RF Weapon by ‘Back Yard’ Methods.* Transcript provided from internet site <http://cryptome.org/rfw-jec.htm>. While materials containing liquid or carbon molecules are quite susceptible to molecular heating, others are not. In addition, molecules only react to frequencies that they absorb. Therefore, matching the right frequency to the material is another difficulty.

¹⁸ Benford, Swegle, and Schamiloglu, 66-68, and Brunderman, 11-12.

¹⁹ Brunderman, 12-13, and Sowders, et al, 81. There are four categories for HPM effects.

“Upset”- a temporary alteration of the electrical state of one or more nodes, precludes normal operation until the radiation is removed. “Lock-up” - same as above, however, an electrical reset, or reboot is necessary to restore normal operation. “Latch-up” - an extreme form of lock-up in which a node is either destroyed or power is cut off to it; “Burnout”- physical destruction of a node where the current becomes so great that the circuitry melts. Similar to what occurs in an appliance after a lightning strike.

²⁰ Brunderman, 14. UWB devices have the majority of their energy in the out-of-band frequencies.

²¹ Benford, Swegle, and Schamiloglu, 235.

²² Geis, *Directed Energy Weapons on the Battlefield*, 9-10. Electric field strengths of three to eight kilovolts per meter can cause lock-up for commercial off-the-shelf equipment requiring a reboot. Seven to 20 kilovolts per meter will cause some equipment to be damaged requiring component repair or replacement. Above 20 kilovolts per meter, damage is probable.

²³ Benford, Swegle, and Schamiloglu, 45-46.

²⁴ Kirk E. Hackett, PhD, e-mail to the author, 8 Dec 2009.

²⁵ Kirk E. Hackett, PhD, e-mail to the author, 8 Dec 2009. Normally the lethal footprint of an HPM weapon is small. One possible design only affects unshielded electronic systems in a 1000 square meter area, or 32 meter by 32 meter square, less than a quarter of a football field. Beam divergence depends on the antenna’s design and aperture size. Directional antennas with large apertures have less angular divergence. See note 29 for further information.

²⁶ Abrams, “Dawn of the E-Bomb,” 27.

²⁷ Benford, Swegle, and Schamiloglu, 46-47.

²⁸ In some cases, this will be easy, like when the power grid fails immediately following an HPM attack. However, in other instances, causality is not straightforward. One cannot be certain that the attack caused the effect if one does not have firsthand knowledge or supporting data. A site can stop emitting because the attack was successful or they turned it off. For example, in both Operations DESERT STORM and ALLIED FORCE, the enemy response to a HARM attack was to turn off the system. There is also the possibility that a site will continue to transmit, but not be functional. The example here is an emitter continues to transmit, but the overall system is not functional because the HPM weapon has disrupted or destroyed the computer that controls the emissions. That is why it is essential to correlate information from multiple sensors and understand systems within systems to determine the exact cause.

²⁹ Nielsen, *Effects of Directed Energy Weapons*, 210, and Kirk E. Hackett, PhD, e-mail to the author, 8 Dec 2009. As HPM radiation emerges from an aperture, it begins to spread out. For a directional antenna, the angular divergence is approximately inversely proportional to the aperture diameter (d), i.e., angular divergence = wavelength/d. For omni-directional antennas like a car radio antenna, beam attenuation is inversely proportional to the square of the antenna's aperture size. Increasing the aperture size increases the antenna's area, decreases the beam's divergence, and therefore concentrates more power on the targeted area. Power or fluence on target is expressed in the formula, $\mathcal{E} = \tau \frac{G P_t}{4\pi R^2} C$. \mathcal{E} is the energy in J/cm², τ is the pulse length in sec, G is the antenna gain (dimensionless and basically the antenna's area times its efficiency), P_t is the transmitter power in Watts, R is the range in cm, and C is an attenuation coefficient (dimensionless) that describes the power lost going through walls or other objects enroute to the target.

³⁰ Beason, 182-184.

³¹ Benford, Swegle, and Schamiloglu, 56-57, and Merritt.

³² This is not the same as OnStar's vehicle slowdown service. OnStar's service has the code to send commands to vehicle's computer and limits the engine output to slow the vehicle whereas an HPM weapon would disrupt or destroy the vehicle's computer and/or ignition system without the code thereby stopping the engine's operation.

³³ Air Force Research Laboratory, *High Power Microwaves Fact Sheet*, 3. Available at <http://www.kirtland.af.mil/library/factsheets/factsheet.asp?id=15869> as of April 9, 2009.

³⁴ David A. Fulghum, "Fried Chips," 29. Initial e-bomb designs were only effective out to 10s of meters.

³⁵ Benford, Swegle, and Schamiloglu, 49-50, "Foreign Help for High Tech Weapons." <http://www.globalsecurity.org/military/library/report/2004/04fisher/Shitech.html>, and Kopp, "Ranets-E High Power Microwave Directed Energy Weapon." Available at <http://www.ousairpower.net/APA-Rus-PLA-PD-SAM.html#Ranets>. The current design of the Ranets-E is on the MAZ-7910 chassis, the same chassis used for the SA-20. The output of the system is speculated to be 500 MW, 10-20 nsec, 500Hz in X-band pulses with a 45-50dB gain antenna. According to the article, this means an effective range to disrupt unshielded COTS electronics between 3.8 to 7.0 nm. The key assumptions here are that the target's electronics are not shielded and field strength of three kilovolts per meter is sufficient. This is at the lower end of the three to eight kilovolts per meter needed to cause lock-up for COTS equipment requiring a reboot.

³⁶ Raytheon Company, "Vigilant Eagle Airport Protection System," 1. "Vigilant Eagle uses a simple technique of illuminating the missile body with electromagnetic energy tailored to divert the missile. When located at a commercial airport, Vigilant Eagle creates a dome of protection around the airport, protecting all aircraft during the most critical phases of flight—takeoff and landing. Vigilant Eagle consists of three major components: a distributed missile detect and track subsystem (MDT), a command and control (C2) system and the Active Electronically Scanned Array, which includes a billboard-sized array of highly efficient antennas linked to solid-state amplifiers."

³⁷ Kopp, "Ranets-E High Power Microwave Directed Energy Weapon." Available at <http://www.ousairpower.net/APA-Rus-PLA-PD-SAM.html#Ranets>.

³⁸ Benford, Swegle, and Schamiloglu, 6.

³⁹ Gulczinski, “Overview of Megawatt Power and Thermal Systems,” Nechev, Erbacher, Vukson, and Christensen, “Lithium Ion Pulse Power Technology,” and Hamilton, “Battery Breakthrough,” 12. Designing the cathodes with nano-materials vastly increases the effective surface area, which equates to more efficient battery output and shorter recharge cycles. The F-35 uses lithium-ion batteries in its current design. These kinds of densities could lead to a 10-fold increase in power output and therefore range. Current battery technology has produced devices in the 500MW to one GW class. So theoretically, this will make five to 10 GW devices possible.

⁴⁰ Curry, O’Connor, and Altgilbers. “A Wideband Megawatt Source.” This is almost a threefold increase over previous designs, which equates to a weapon having an effective radius against unshielded electronics of 70 meters or covering an area equal to 3.5 football fields.

⁴¹ Kirk E. Hackett, PhD, interview by the author, 13 Nov 2009, and McCarthy, *Directed Energy and Fleet Defense*, 25-26.

⁴² Benford, Swegle, and Schamiloglu, 6-7, and Bracken, “Technological Innovation and National Security.”

⁴³ The most promising designs are multi-wave generators, and relativistic klystrons, magnetrons and diffraction generators, as well as advances to older systems like the magnetic insulated line oscillator (MILO), vircators, and impulse-radiating antenna (IRA). It is beyond the scope of this paper to go into the technical details of each of these microwave sources. One can find a thorough discussion on each type of microwave generator in the following sources. James Benford, John A. Swegle, and Edl Schamiloglu, *High Power Microwaves*, 2nd ed. (Boca Raton, FL: CRC Press, Taylor and Francis Group, 2007), Chapters 7-10, and Steven H. Gold, Gregory S. Nusinovich, “Review of High-Power Microwave Source Research,” *Review of Scientific Instruments* 68, no. 11 (November 1997): 3945-3974

⁴⁴ Air Force Research Laboratory, *High Power Microwaves Fact Sheet*, 3.

⁴⁵ Benford, Swegle, and Schamiloglu, 4-10, and Air Force Research Laboratory, *High Power Microwaves Fact Sheet*, 2-3. In simple terms, phase locking focuses the outputs of several antennas into a coherent wave by putting each wave in sync and aimed at the same point. This allows lower power transmissions from several apertures thereby minimizing atmosphere breakdown, but when combined, they increase the power on the target. Similar technology is already used in active electronically scanned radars where numerous solid-state transmitter/receivers are combined to form a coherent beam.

⁴⁶ Fulghum, “Fried Chips,” 28-29, and Fulghum, “Lasers, HPM Weapons near Operational Status,” 173.

⁴⁷ Bertin, “Critical Directed Energy Test and Evaluation Infrastructure Shortfalls,” Locke, “Blackout Bomb,” 24-25, Fulghum, “Fried Chips,” 28-29, Fulghum, “Lasers, HPM Weapons near Operational Status,” 173, and Barrie, “Focused Effort,” 39. According to these articles, the U.S., UK, and Israel are researching HPMs for anti-missile applications, and payloads for cruise missiles and UCAVs. USAF researchers plan to start tests with the U.S. prototype UCAV, CHAMP, beginning in 2012.

⁴⁸ United States Defense Science Board, *Defense Science Board Task Force on Directed Energy Weapons*, 1-4, 52-53, and Clay Wilson, *High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices*, 21-22.

⁴⁹ Clay Wilson, *High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices*, 11-12. “The study concluded that an EMP attack affecting the Baltimore-

Washington-Richmond region could result in economic output loss potentially exceeding \$770 billion, or 7 percent of the nation's annual gross domestic product. Even under the most favorable assumptions, including both shielded and unshielded critical infrastructure, an EMP might still result in damage that would require one month of recovery and economic loss of \$9 billion and \$34 billion respectively. In the worst case, according to the study, not only is the damage from EMP widespread, but the duration of disrepair lasts for years. In such cases, there are numerous complicating factors that could slow the recovery process."

⁵⁰ United States Defense Science Board, *Defense Science Board Task Force on Directed Energy Weapons*, 1-4, and Clay Wilson, *High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices*, 4-12.

⁵¹ Bertin, "Critical Directed Energy Test and Evaluation Infrastructure Shortfalls," and Kirk E. Hackett, PhD, interview by the author, 13 Nov 2009. "The difficulty with hardening is that one needs to know the coupling paths for energy into systems. Unlike for more traditional electronic warfare, where side-lobes and front door attacks are used, HPM energy couples through power, keyboard, mouse cables, air vents, thru plastic panels covering hard drives, etc. Only through testing can one be sure systems are hardened." All services are investigating HPM weapons and defenses to counter these weapons. However, up to now, there has been very little research into the vulnerabilities of current U.S. systems. For example, the F-16 is the only operational USAF aircraft to have undergone even limited vulnerability tests. One of the 52 multiservice shortfalls briefed at the 11th Annual Directed Energy Symposium was the inability to protect systems and key subsystems during HPM testing. Vulnerability testing is difficult, potentially destructive, and costly, but is necessary. One solution that the Air Force Research Laboratory's Directed Energy Directorate is working on is to improve modeling and simulation.

⁵² Asmontas, Gradauskas, Suziedelis, Kozic, Paskevic, Kazlauskaite, and Sirmulis, "Microwave to Terahertz Radiation Detection by Semiconductor Nanostructures," Žurauskienė, Balevičius, Stankevič, Keršulis, Abrutis, Plaušnaitienė, and Altgilbers, "La-Sr(Ca)-MnO₃ Films for a Fast Room Temperature Symmetrical Fault Current Limiter," and Benford, Swegle, and Schamiloglu, 64.

⁵³ Clay Wilson, *High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices*, 14. To harden most military systems and mass-produced commercial equipment adds two to three percent to the total cost. To retro-harden existing electrical equipment adds about three to ten percent to the total cost.

⁵⁴ United States. Department of the Air Force. Scientific Advisory Board, *New World Vistas*, 60.

⁵⁵ Geis, 36. The current generation of officers is not trained to operate without automation and information technology. One example is primary pilot training where students are using GPS for navigation from their first flight and have difficulty navigating without it. Another example is joint air operations. The entire system from the air operations center to the individual units is dependent on the Theater Battle Management Control System (TBMCS) and other systems to plan and operate. Military units do not exercise to operate without this connectivity.

⁵⁶ Givri, 30.

⁵⁷ T. V. Paul, "Complex Deterrence: An Introduction," in *Complex Deterrence: Strategy in the Global Age*, ed. T. V. Paul, Patrick M. Morgan, and James J. Wirtz. (Chicago, IL: University of Chicago Press, 2009), 2-3

⁵⁸ John J. Mearsheimer, *Conventional Deterrence*, (Ithaca: Cornell University Press, 1983), 14.

⁵⁹ Paul, 2.

⁶⁰ Jeffrey W. Knopf, “Three Items in One: Deterrence as Concept, Research Program, and Political Issue,” in *Complex Deterrence: Strategy in the Global Age*, ed. T. V. Paul, Patrick M. Morgan, and James J. Wirtz. (Chicago, IL: University of Chicago Press, 2009), 31-54, and Janice Gross Stein, “Rational Deterrence against Irrational Adversaries: No Common Knowledge,” in *Complex Deterrence: Strategy in the Global Age*, ed. T. V. Paul, Patrick M. Morgan, and James J. Wirtz. (Chicago, IL: University of Chicago Press, 2009), 58-80.

⁶¹ Benford, Swegle, and Schamiloglu, 9-12, and United States Defense Science Board, *Defense Science Board Task Force on Directed Energy Weapons*, 40.

⁶² United States Defense Science Board, *Defense Science Board Task Force on Directed Energy Weapons*, 36-40, and Clay Wilson, *High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices*, 21-22.

⁶³ HMP attacks can range from temporary upset of a single computer to the permanent destruction of a large segment of the national infrastructure. Covering all the gradations in-between is not practical.

⁶⁴ For this discussion, a catastrophic attack poses an existential threat, or can cause irreparable damage to the U.S. economy and/or political systems, or result in mass casualties.

⁶⁵ For more on the meaning of conventional deterrence see: Alexander L. George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (New York, NY: Columbia University Press, 1974); Richard Ned Lebow, *Between Peace and War: The Nature of International Crisis* (Baltimore, MD: Johns Hopkins University Press, 1981); Robert Jervis, Richard Ned Lebow and Janice Gross Stein, eds., *Psychology and Deterrence* (Baltimore, MD: Johns Hopkins University Press, 1985). Readers desiring a shorter synopsis can read T.V. Paul, Patrick Morgan and James Wirtz (eds), *Complex Deterrence: Strategy in the Global Age* (Chicago, IL: University of Chicago Press, 2009).

⁶⁶ Clay Wilson, *High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices*, 11-12.

⁶⁷ Clay Wilson, *High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices*. For further information on HEMP attacks, reference the EMP Commission Reports of 2004 and 2008.

Bibliography

- Abrams, Michael. "Dawn of the E-Bomb." *IEEE Spectrum* 40, no. 11 (November 2003): 24-30.
- Asmontas, S., J. Gradauskas, A. Suziedelis, A. Kozic, C. Paskevic, V. Kazlauskaite, and E. Sirmulis. "Microwave to Terahertz Radiation Detection by Semiconductor Nanostructures." Research Report Presented at the Tenth Annual Directed Energy Symposium. Huntsville, AL, November 2007.
- Barnes, Paul N., Gregory L. Rhoads, Justin C. Tolliver, Michael D. Sumption, and Kevin W. Schmaeman. "Compact, Lightweight, Superconducting Power Generators." *IEEE Transactions on Magnetics* 41, no. 1 (January 2005): 268-273.
- Beason, Doug, Ph.D. *The E-Bomb: How America's New Directed Energy Weapons Will Change the Way Future Wars Will Be Fought*. Cambridge, MA: Da Capo Press, 2005.
- Barrie, Douglas. "Focused Effort." *Aviation Week & Space Technology* 167, no. 8 (20 August 2007): 39.
- Benford, James, John A. Swegle, and Edl Schamiloglu. *High Power Microwaves*. 2nd ed. Boca Raton, FL: CRC Press, Taylor and Francis Group, 2007.
- Bertin, Michael S. "Critical Directed Energy Test and Evaluation Infrastructure Shortfalls: Results of the DETEC Tri-Service Study Update." Briefing. Eleventh Annual Directed Energy Symposium, 18 November 2008.
- Bracken, Paul. "Technological Innovation and National Security." Foreign Policy Research Institute, June 2008.
<http://www.fpri.org/enotes/200806.bracken.innovationnationalsecurity.html>.
- Brunderman, Lieutenant Colonel John A. "High Power Radio Frequency Weapons: A Potential Counter to U.S. Stealth and Cruise Missile Technology." Research Paper, Center for Strategy and Technology, Air University, December 1999.
- Curry, Randy D., Kevin O'Connor, and Larry Altgilbers. "A Wideband Megawatt Source Driven by an Explosive Flux Compression Generator." Briefing. Tenth Annual Directed Energy Symposium, 6 November 2007.
- Dougherty, Lieutenant Colonel Brian K. "Airborne Directed Energy Weapon Applications for Special Operations Forces." Research Paper, Center for Strategy and Technology, Air University, April 2004.
- Durham, Will. "U.S. May Debut Secret Microwave Weapon versus Iraq."
<http://www.globalsecurity.org/org/news/2003/030202-ebomb01.html>.

Fager, Major Chadwick F. “Weaponizing the Future: Direct Energy Weapons Effectiveness Now and Tomorrow.” Maxwell AFB, AL, Air Command and Staff College, 2007.

“Foreign Help for High Tech Weapons.”

<http://www.globalsecurity.org/military/library/report/2004/04fisher/5hitech.html>

(accessed 3 November 2009).

Fulghum, David A. “EMP Weapons Lead Race for Non-Lethal Technology.” *Aviation Week & Space Technology* 138, no. 21 (24 May 1993): 61.

Fulghum, David A. “Fried Chips.” *Aviation Week & Space Technology* 169, no. 15 (20 October 2008): 28-29.

Fulghum, David A. “Lasers, HPM Weapons near Operational Status.” *Aviation Week & Space Technology* 157, no. 4 (22 July 2002): 173.

Fulghum, David A. “Silent Launch.” *Aviation Week & Space Technology* 165, no. 4 (24 July 2006): 66.

Geis, Lieutenant Colonel John P. *Directed Energy Weapons on the Battlefield: A New Vision for 2025*. Occasional Paper No. 32. Maxwell AFB, AL: Center for Strategy and Technology, Air University Press, April 2003.

George, Alexander L., and Richard Smoke. *Deterrence in American Foreign Policy: Theory and Practice*. New York, NY: Columbia University Press, 1974.

Gibilisco, Stan. *Physics Demystified*. New York, NY: McGraw Hill, 2002.

Givri, D. V. *High-Power Electromagnetic Generators: Nonlethal Weapons and Other Applications*. Cambridge, MA: Harvard University Press, 2004.

Gold, Steven H., Gregory S. Nusinovich. “Review of High-Power Microwave Source Research.” *Review of Scientific Instruments* 68, no. 11 (November 1997): 3945-3974.

Gulczynski, Frank, PhD. “Overview of Megawatt Power and Thermal Systems.” Briefing. Tenth Annual Directed Energy Symposium, 6 November 2007.

Hamilton, Tyler. “Battery Breakthrough?” *Technology Review*, 22 January 2007.
<http://www.technologyreview.com/biztech/18086/>.

Hecht, Jeff. *Beam Weapons: The Next Arms Race*. Plenum Press: New York and London, 1984.

Hymes, Colonel Kirk. “Non-Lethal Weapons in Escalation of Force Operations and the Role of Directed Energy.” Briefing. Tenth Annual Directed Energy Symposium, 6 November 2007.

- Jackson, Lieutenant Colonel Jack A., Jr., PhD, Lieutenant Colonel Brian L. Jones, PhD, Major Lee J. Lehmkuhl. "An Operational Analysis for Air Force 2025: An Application of Value-Focused Thinking to Future Air and Space Capabilities." *Air Force 2025 Final Report*. <http://csat.au.af.mil/2025/volume4/vol4ch03.pdf>.
- Jersey, Major Sean L. "Twenty First Century Weapons: Theater Operation at the Speed of Light." Research Paper, Naval War College, February 2003.
- Jervis, Robert, Richard Ned Lebow, and Janice Gross Stein, eds. *Psychology and Deterrence*. Baltimore, MD: Johns Hopkins University Press, 1985.
- Kopp, Carlo. "The Electromagnetic Bomb: A Weapon of Electrical Mass Destruction." *Air and Space Power Journal*, Chronicles Online Journal (1996).
<http://www.airpower.maxwell.af.mil/airchronicles/cc/apjemp.html>.
- Kopp, Carlo. "Hardening Your Computing Assets."
www.globalsecurity.org/military/library/report/1997/harden.pdf.
- Kopp, Carlo. "Ranets-E High Power Microwave Directed Energy Weapon." *Air Power Australia*, 31 May 2008. <http://www.ausairpower.net/APA-Rus-PLA-PD-SAM.html#Ranets>.
- Lebow, Richard Ned. *Between Peace and War: The Nature of International Crisis*. Baltimore, MD: Johns Hopkins University Press, 1981.
- Liang, Qiao, and Wang Xiangsui. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House, February 1999. <http://www.terrorism.com/documents/TRC-Analysis/unrestricted.pdf>.
- Lorber, Azriel. *Misguided Weapons: Technological Failure and Surprise on the Battlefield*. Dulles, VA: Potomac Books, Inc., 2002.
- Locke, Susannah F. "Blackout Bomb." *Popular Science* 275, no. 2 (August 2009): 24-25.
- Major, Aaron. "Which Revolution in Military Affairs? Political Discourse and the Defense Industrial Base." *Armed Forces & Society* 35, no. 2 (January 2009): 333-361.
- McCarthy, Captain William J. *Directed Energy and Fleet Defense: Implications for Naval Warfare*. Occasional Paper No. 10. Maxwell AFB, AL: Center for Strategy and Technology, Air University Press, May 2000.
- Mearsheimer, John J. *Conventional Deterrence*. Ithaca, NY: Cornell University Press, 1983.

- Nechev, Kamen, John Erbacher, Stephen Vukson, and Brent Christensen. "Lithium Ion Pulse Power Technology for Intermediate Energy Storage." Briefing. Tenth Annual Directed Energy Symposium, 6 November 2007.
- Neuber, A., A. Young, M. Elsayed, J. Dickens, M. Giesselmann, M. Kristiansen, and L.L. Altgilbers. "Compact High Power Microwave Generation." Texas Tech University, 2008. <http://www.asc2008.com/manuscripts/D/DO-03.pdf>.
- Nielsen, Philip E. *Effects of Directed Energy Weapons*. Albuquerque, NM: Directed Energy Professional Society, 2009.
- Paul, T. V., Patrick M. Morgan, and James J. Wirtz, eds. *Complex Deterrence: Strategy in the Global Age*. Chicago, IL: University of Chicago Press, 2009.
- Raytheon Company. "Vigilant Eagle Airport Protection System: Ground-Based Counter-MANPADS Protection for Large Airports and Air Bases." Product Data Sheet. Tucson, AZ: Raytheon Company Missile Systems, Directed Energy Weapons, 2006-2008.
- Rodgers, J., M.A. Holloway, T. M. Firestone, and V. L. Granatstein. "HPM Effects in Advanced Electronics." Briefing. Tenth Annual Directed Energy Symposium, 6 November 2007.
- Rose, Rebecca. "AFOSR-Sponsored Researcher Develops New Type of Magnetron." Air Force Office of Scientific Research, Wright-Patterson Air Force Base, 21 September 2009. <http://www.wpafb.af.mil/news/story.asp?id=123167173>.
- Shotts, Zac. "Design Methodology for Dual Resonance Pulse Transformers." Briefing. Tenth Annual Directed Energy Symposium, 6 November 2007.
- Sowders, Captain David M, et al. *High Power Microwave (HPM) and Ultrawideband (UWB): A Primer on High Power RF*. Special Report from Phillips Laboratory. Advanced Weapons and Survivability Directorate. Kirtland AFB, NM: Air Force Materiel Command, March 1996.
- Theury, Jacques. *Microwaves: Industrial, Scientific, and Medical Applications*. Norwood, MA: Artech House, Inc., 1992.
- United States Congress. *Joint Economic Committee Hearing: Radio Frequency Weapons and Proliferation: Potential Impact on the Economy*. Opening statements of James O'Bryon, David Schriener, Dr. Ira Merritt, and Dr. Alan Kehs. 105th Congress, 25 February 1998.
- U.S. Congress. *Joint Economic Committee Hearing: Economic Espionage, Technology Transfers and National Security*. Opening Statement of Lt. Gen. Robert L. Schweitzer, U.S. Army (Ret). 105th Congress, 17 June 1997.

- United States. Defense Science Board. Task Force on Directed Energy Weapons and United States Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. *Defense Science Board Task Force on Directed Energy Weapons*. Washington D.C.: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, December 2007. http://www.acq.osd.mil/dsb/reports/2007-12-Directed_Energy_Report.pdf.
- United States. Department of the Air Force. Air Force Research Laboratory. *High Power Microwaves Fact Sheet*. Kirtland AFB, NM: Air Force Research Laboratory, Office of Public Affairs, 9 April 2009.
- United States. Department of the Air Force. Scientific Advisory Board. *New World Vistas: Air and Space Power for the 21st Century: Directed Energy Volume*. Washington, D.C.: USAF Scientific Advisory Board, 1995. <http://handle.dtic.mil/100.2/ADA309595>.
- Varni, Lieutenant Colonel Jamie G. G., Gregory M. Powers, Major Dan S. Crawford, Major Craig E. Jordan, and Major Douglas L. Kendall. "Space Operations: Through the Looking Glass (Global Area Strike System)." *Air Force 2025 Final Report*. <http://csat.au.af.mil/2025/volume3/vol3ch14.pdf>.
- Walling, Colonel Eileen M. *High Power Microwaves: Strategic and Operational Implications for Warfare*. Occasional Paper No. 11. Maxwell AFB, AL: Center for Strategy and Technology, Air University Press, May 2000.
- Wilson, Clay. *High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessments*. CRS Report for Congress. Washington D.C.: Congressional Research Service, 21 July 2008.
- Wilson, Clay. *Information Warfare and Cyberwar: Capabilities and Related Policy Issues*. CRS Report for Congress. Washington D.C.: Congressional Research Service, 19 July 2004.
- Wilson, Tom. "Threats to United States Space Capabilities." Report Prepared for the Commission to Assess United States National Security Space Management and Organization. January 2001.
- Zhihao, Zhu. *Trends of Microwave Weapon Development*. Translated by Edward A. Suter. WPAFB, OH: National Air and Space Intelligence Center, 4 January 1996.
- Žurauskienė, N., S. Balevičius, V. Stankevič, S. Keršulis, A. Abrutis, V. Plaušinitienė, and Larry L. Altgilbers. "La-Sr(Ca)-MnO₃ Films for a Fast Room Temperature Symmetrical Fault Current Limiter." Research Report Presented at the Tenth Annual Directed Energy Symposium. Huntsville, AL, November 2007.